Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 29 (2012) 3483 – 3486

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Workshop on Information and Electronics Engineering (IWIEE)

Delaying Function Construction Based on Triple DES

Ye Yingze[a], Zhang Ying[b*]

[a]*Modern Education Technology Center,HuaZhong Agricultural University,Wuhan,China*
Corresponding Author[b]:Department of Computer Science,College of Science,HuaZhong Agricultural University,Wuhan,China

Abstract

Delaying function refers to a type of function where the output of the function requires some time, with computational complexity different from cipher. This paper gives a method of realizing delaying function based on hash collision and the delaying function realized by this method is characterized by safety, high-efficiency and controllable delay. This approach can be applied to the generation of winning numbers of e-lottery ticket, which is beneficial for the design of e-lottery scheme.

Keywords:delaying function; triple DES; hash function; hash collision

1. Introduction

The development of Internet promotes the Internet-based e-business, in which e-lottery ticket constitutes a major part. Due to the extensive distribution of terminals for lottery ticket sales, the time synchronization for sales terminals is quite difficult to achieve. After the generation of winning numbers, sales terminals can forge lottery tickets by utilizing the time difference to cheat the prize money. To prevent such fraud, delaying function is proposed[1], and it has been widely applied in the generation of winning numbers of e-lottery ticket to restrict unfairness caused by failure in time synchronization [2][3]. In all of the literatures mentioned above, only the concept of delaying function is proposed, without presenting the examples on how to realize delaying function. Therefore, the doubt regarding the existence of delaying function has long been prevalent. This paper, based on Triple DES, constructs hash function

* Corresponding author. Tel.: 15307115201
E-mail address: zy@mail.hzau.edu.cn.

1877-7058 © 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2012.01.516

which can be quickly realized, and the delaying function is further constructed based on the collision of hash function. Delaying function constructed using hash collision based on triple DES has the advantages of safety, high efficiency and controllable delay. Our study is significant for the design of e-lottery scheme as well as the application of delaying function in other fields of e-business.

2. Brief introduction of delaying function

Literature [1] proposes the concept of delaying function. Delaying function is a type of function generating the output after some time, with moderate computational complexity, though the complexity is different from that of the cipher. To be delaying function, a function f should satisfy the following two conditions:

- (1) f is difficult to calculate. At the shortest calculation time p and time interval q given, the probability to complete the calculation of f is no greater than (arbitrarily small) within [p, q]. This is the requirement of the calculation time or the delay.
- (2) The quantity of output information is equal to that of input information. Let Y=f(X), then we have H(X) = H(Y), where H(X) is the entropy of X [4]. As delaying function is frequently applied in generating random numbers, keeping entropy constant is a basic requirement in order to ensure the randomness of the output of delaying function.

Without delaying function in the design of e-lottery scheme, the lottery fraud after the generation of winning numbers is possible by taking advantage of the failure in time synchronization at the sales terminals as the clocks at the sales terminals do not reach the closing time for lottery sales. That means the lottery ticket can be forged after the winning numbers has come out. To prevent fraud, many lottery design schemes use the concept of delaying function, but they do not present the method of designing the specific delaying function. The design of delaying function in this paper complies with the following principles:

- (1) Easy implementation scheme;
- (2) High security;
- (3) Controllable delay time.

3. Hash collision

Hash function in cryptography maps information M of arbitrary length into hash value of fixed length. Hash function has the following properties:

- (1) For arbitrarily given x, hash(x) is relatively easy to calculate;
- (2) For arbitrarily given h, x is searched to make it infeasible to calculate h=hash(x);
- (3) For arbitrarily given x, y is searched to make the calculation of hash(x) = hash(y) infeasible;
- (4) For arbitrary (x, y), the calculation of hash(x) = hash(y) is made infeasible.

Property (3) and (4) are the collision resistance of hash function, which determines the security of hash function to a considerable extent. The attack against hash function is mainly realized by seeking data pair for hash collision. Currently, the attacks against any type of hash function are birthday attack [5] and differential attack [6]. In birthday attack, the structure of hash function and any of its weak algebraic properties are not utilized. Rather, birthday attack only depends on the length of information abstract, i.e., the length of hash value. When the length of hash value is ε, a collision is generated through an average of $\sqrt{n}$ operations.

4. Design of delaying function based on triple DES

In January of 1977, US government adopted Data Encryption Standard (product cipher) developed by IBM as non-confidential information. This action encouraged a large number of manufacturers to develop the encryption algorithm for data encryption standard in confidential industry [7]. DES algorithm, as a block encryption algorithm, comprehensively uses multiple encryption techniques, including replacement, substitution and algebraic technique. By dividing information into 64-bit block, the 56-bit key is used with the iteration count of 16. This algorithm has a 64-bit key as the parameter, and in DES algorithm, 8 parity bits of the 64-bit initial key are eliminated, leaving behind the 56-bit initial key. The original information is divided into 64-bit data block of fixed length. Then, using 56-bit encryption key, 64-bit encrypted information is generated by substitution and combination method. The decryption key is the same with encryption key, but with the reverse steps. Using encryption method, DES encrypts one bit or one byte at a time, generating the stream cipher. For DES, the number of available encryption keys is 256. DES algorithm has been extensively applied, and it is regarded as highly reliable in theory. Until now, no effective attack algorithm has been found besides exhaustive attack. However, considering the current operating speed of computer, the defect of DES is also obvious, i.e. the too short length of 56-bit key. To avoid the potential safety hazard caused by the short length of key, DES is extended to triple DES. That is, key K1 is first used to encrypt DES, and then the cipher text is decrypted with K2. Finally, K1 is used for the second time to encrypt the decrypted data once more. This method is equivalent to encrypting the plain text data using 112-bit key K1|| K2 (|| indicates the connection of bits). In this way, the keyspace is extended from 256 to 2112, which greatly improves its safety.

Based on Triple DES algorithm, hash function is designed. Let $h(x) = [Triple\_DES_x(v_0)]_{(1...n)}$, where x= K1|| K2 is Triple-DES key and v0 is the encrypted data in Triple DES (in this scheme, v0 is fixed). Figure 1 shows Triple DES encryption with x as the key and v0 as the output. The outputs of triple DES encryption operations are denoted as v1, v2 and v3. Let $Triple\_DES_x(v_0) = v_1 \,||\, v_3$, where || indicates the connection; $[Triple\_DES_x(v_0)]_{(1...n)}$ indicates that low-order n bits of the output of $Triple\_DES_x(v_0)$ is taken as the output of h(x). The value of n is determined by the requirement of delay time and the calculation capacity. Hash function $h(x) = [Triple\_DES_x(v_0)]_{(1...n)}$ satisfies the requirements specified previously, i.e. unidirectionality and collision resistance. Based on hash function $h(x) = [Triple\_DES_x(v_0)]_{(1...n)}$, delaying function is defined as y=D(x),where y is exhaustively searched in key space with the size of 2112 to make h(x)=h(y), that is triple DES collision is searched. According to the requirements of time delay and the computation capacity, different n is selected. When shorter delay time is needed, smaller n is selected; while in the case of longer delay time, larger n is selected. Also, the value of n selected is increased with the increase in computation capacity. By this means, the optimal combination of resources and efficiency can be achieved.

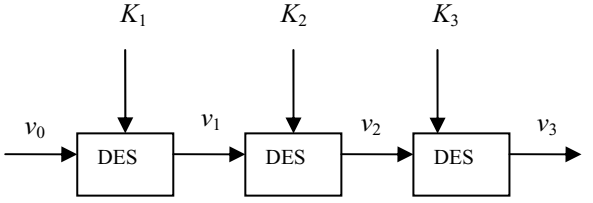

Fig. 1. Drawing of Triple-DES structure

5. Summary

In this paper, we present the design of delaying function based on triple DES. Keyspace of triple DES has the size of 2112, with greater security. The realization of DES is also simple and highly efficient. Our hash function $h(x) = [Triple\_DES_x(v_0)]_{(1...n)}$ generates hash value with the greatest length of 128 bits. Based on the result of birthday attack, 264 operations are needed for one pair of collision. When shorter delay time is needed, smaller value of n should be selected. At n=64, only 232 operations are needed to generate one pair of collision. Delaying function based on triple DES designed in this paper has good security performance, with simple realization method and controllable delay. As it satisfies all of the requirements previously mentioned, this function is applicable to safe e-business.

Acknowledgements

This work was financially supported by the Fundamental Research Funds for the Central Universities (Program No. 2011JC018).

References

[1] D. M. Goldschlag and S. G. Stubblebine. Publicly Verfiable Lotteries. Applications of Delaying Functions. FC'98，LNCS 1465,1998:214~226

[2] E．Kushilevitz and T. Rabin. Fair e-Lotteries and e-Casinos. CT-RSA 2001，LNCS 2020,2001:100~109

[3] Sher S. M. Chow，Lucas C. K. Hui, S. M. Yiu and K. P. Chow. An e-Lottery Scheme Using Verifiable Random Function . ICCSA2005, LNCS 3482,2005:651~660

[4] Robert J．McEliece．Information theory and coding theory(Second Edition)[M]．Publishing House of electronics industry,2004:13~15

[5] Paul C van 00rschot, Michael J Wiener. Parallel Collision search with Cryptanalytic Applications[J]. Journal of Cryptology, 1999,(12):l~28

[6] H Dobbertin. cryptanalysis of MD4．FSE96,1996:53~69

[7] National Institute of standards and Technology(NIST)．FIPS publication 46-2:Data Encryption Standard(DES), 1976